LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

TCEMG

TRIBUNAL DE CONTAS DO ESTADO DE MINAS GERAIS

Tribunal de Contas do Estado de Minas Gerais

Presidente
Conselheiro Mauri José Torres Duarte

Vice-Presidente
Conselheiro Gilberto Pinto Monteiro Diniz

Corregedor
Conselheiro Durval Ângelo Andrade

Ouvidor
Conselheiro Wanderley Geraldo de Ávila

Conselheiros
Cláudio Couto Terrão
José Alves Viana

Conselheiro em Exercício
Adonias Fernandes Monteiro

Conselheiros Substitutos
Licurgo Joseph Mourão de Oliveira
Hamilton Antônio Coelho
Adonias Fernandes Monteiro
Telmo de Moura Passareli

Ministério Público junto ao Tribunal de Contas

Procurador-Geral
Marcílio Barenco Corrêa de Mello

Subprocurador-Geral
Daniel de Carvalho Guimarães

Procuradores
Maria Cecília Mendes Borges
Glaydson Santo Soprani Massaria
Elke Andrade Soares de Moura
Sara Meinberg Schmidt de Andrade Duarte
Cristina Andrade Melo

Expediente

Realização

Diretoria de Comunicação
Luiz Cláudio Diniz Mendes | Diretor

Coordenadoria de Publicidade e Marketing
André Augusto Costa Zocrato | Coordenador

André Luiz de Oliveira Junior
Bruna Gontijo Pellegrino
Giovana Fernandes Almeida
Lívia Maria Barbosa Salgado
Vinícius Barbosa Dias
Vivian de Paula

Elaboração
Giovana Fernandes Almeida

Núcleo de Proteção de Dados
Luiza Amâncio Ferreira Duarte | Encarregada de Dados

Clara Amédée Péret Motta
Paulo Jorge Teixeira Nunes

Supervisão de Segurança Institucional da Informação
Gustavo Mendes Guimarães
Flávio Régis Carvalho de Moura Castro
Tadeu Antônio Santiago Vieira

SUMÁRIO

LGPD

A Constituição Federal de 1988 estabelece quais são os direitos fundamentais. Entre eles podemos citar a intimidade, a vida, a honra, a imagem, a liberdade e recentemente foi incluída a proteção dos dados pessoais, especialmente em meios digitais.

E por que essa inclusão é tão importante? Estamos em uma era em que o processamento de dados assumiu um papel muito grande no ambiente econômico. Nossos dados são utilizados em inúmeras plataformas e, baseado em nosso perfil de consumo, várias publicidades são direcionadas conforme nossas preferências. Isso significa dizer que nossos dados se tornaram extremamente valiosos para as empresas.

Entretanto, essa coleta de dados, atualmente realizada de forma indiscriminada, tem trazido desconforto e insegurança, haja vista que para qualquer atividade realizada pelo titular, há sempre um pedido de preenchimento de cadastro. Mas, qual a finalidade? Para quê os meus dados estão sendo coletados? Uma simples compra, à vista, requer que informemos nosso nome, endereço de e-mail, data de aniversário, CPF.... Tudo isso realmente é necessário para que apenas possamos adquirir um produto? Ou há outras intenções? É possível chegar a uma farmácia, por exemplo, sem que alguém lhe pergunte qual seu CPF? Por quantas vezes um aplicativo nos pede para identificar

nosso local? Essa coleta de dados consegue identificar, inclusive, os nossos hábitos e rotina, o que ajuda no direcionamento de propagandas.

Mas isso é ruim? Se pensarmos que o nosso perfil de consumo está sendo mapeado e por esta razão podemos receber informações e publicidades baseadas apenas sobre o que gostamos e procuramos, isso não é ruim, já que assim teremos acesso a serviços e produtos mais adequados. Entretanto, o que se questiona são os abusos e a falta de transparência das empresas.

Realizar um cadastro em uma empresa para receber informações de determinado item não significa dizer que autorizamos empresas a nos ligarem ou oferecerem ofertas de créditos, por exemplo.

Nesse contexto surgiu a Lei Geral de Proteção de Dados, não para eliminar a coleta e o compartilhamento de dados, mas disciplinar como esses dados podem e devem ser utilizados, respeitando os limites impostos pelos direitos dos titulares e promovendo a necessária transparência das empresas nas relações.

Para muitos a Lei Geral de Proteção de Dados, ou simplesmente LGPD, é desconhecida. Essa cartilha pretende explicar a LGPD de maneira simples e didática, apresentando os conceitos básicos e instigando as pessoas que tratam dados pessoais a pensar como devem realizar o tratamento da melhor maneira. O Núcleo de Proteção de Dados do Tribunal busca conscientizar e treinar os servidores quando do manuseio dos dados, além de servir de auxílio para todos aqueles que tenham interesse em conhecer mais sobre a Lei.

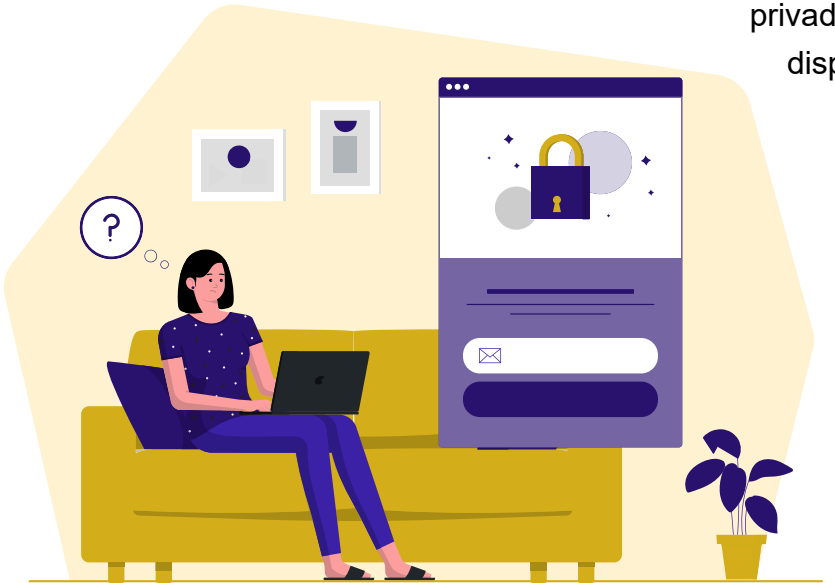
Núcleo de Proteção de Dados

O QUE É A LGPD?

A Lei Geral de Proteção de Dados Pessoais, ou LGPD, regula o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou jurídica de direito público ou privado, visando proteger direitos fundamentais, como a liberdade, a privacidade, e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD confere mais segurança jurídica aos titulares de dados bem como a todos que lidam com informações pessoais no desenvolvimento de suas atividades de negócio.

Seu principal foco é oferecer ao titular dos dados maior conhecimento, controle e transparência na coleta, processamento, uso e compartilhamento de suas informações pessoais. Isso faz valer um dos fundamentos da Lei que é a autodeterminação informativa, ou seja, o poder que cada cidadão tem sobre seus próprios dados, tanto daqueles armazenadas em bancos de dados das instituições privadas e de órgãos públicos quanto dos disponíveis em meios físicos.



A QUEM A LEI SE APLICA?

A LGPD se aplica a toda pessoa natural ou jurídica de direito público ou privado que realize tratamento de dados em território nacional, seja por meio físico ou digital.

Também é aplicada às atividades de tratamento que tenham por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados em território nacional. Exemplo: hotéis argentinos que divulgam seus serviços para o público brasileiro devem se adequar à LGPD.

Outra aplicação da Lei são os dados que foram coletados no território nacional. Isso significa dizer que se uma empresa, ainda que não tenha sede no Brasil, tiver coletado os dados aqui, deve estar adequada à Lei.

ATENÇÃO!

A Lei não é aplicável às pessoas físicas que usam dados pessoais com finalidades particulares e não econômicos, nem para fins exclusivamente jornalísticos, artísticos, acadêmicos, de segurança pública, de defesa nacional ou para atividades de investigação e repressão de infrações penais.

CONCEITOS BÁSICOS

Autodeterminação informativa é a garantia do titular de ter o controle sobre suas próprias informações, ainda que o tratamento dessas informações seja legítimo e não dependa de sua autorização prévia.

Titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, sendo que, como a existência da pessoa natural termina com a morte, só é tido como titular a pessoa viva. Você é o titular de seus dados pessoais e é o principal interessado em saber como eles estão sendo utilizados.

Dados pessoais são todas e quaisquer informações que identificam ou possam identificar uma pessoa natural, como nome, CPF, endereço, e-mail, identidade, idade, telefone, número de matrícula na academia, cor de cabelo, renda, entre outros. Observem que deixamos nossos dados em diversos locais, como cadastro para cursos, registros de navegação de sites de internet, cadastro para acessar sistemas.No âmbito do TCEMG, temos dados corporativos, dos servidores, dos contratados e do público externo com o qual o TCEMG se relaciona, seja jurisdicionado ou cidadão.

Dados pessoais sensíveis são dados pessoais que receberam um cuidado especial pela Lei por poderem causar alguma discriminação ao titular se tratados indevidamente. São eles: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Prontuários médicos são exemplos de coleta de dados pessoais sensíveis.

Tratamento é toda operação realizada com dados pessoais, como coleta, acesso, armazenamento, eliminação e transferência, entre outros.

Dados anonimizados são aqueles relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O dado perde o caráter pessoal, inclusive a associação, direta ou indireta, a um indivíduo, não sendo possível, por meios técnicos e outros, que se reconstrua o caminho para «descobrir» quem era a pessoa titular do dado. Caso contrário, se tratará de um dado pseudoanonimizado.

Um exemplo de dados anonimizados são os dados estatísticos, comumente usados em pesquisas de opinião pública.

Controlador é a pessoa que decide como, quando e por quê tratar os dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado.

Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador de acordo com suas instruções.

Ainda há bastante dificuldade na interpretação de quem é o controlador e quem é operador dependendo do tratamento realizado, mas uma das perguntas que precisam ser feitas é: de quem é o poder de decisão sobre o tratamento? Quem define a finalidade, natureza dos dados e duração do tratamento? Respondendo a essas

perguntas você identifica o controlador.

Mas vale ressaltar que há hipóteses de co-controladores, em que há mais de um controlador sob os mesmos dados pessoais e estes definem conjuntamente as finalidades e os meios do tratamento. É o que acontece em alguns Termos e Acordos de Cooperação Técnica realizados pelo Tribunal com outros órgãos públicos.

Encarregado de dados é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, devendo ter seus dados divulgados publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Banco de dados é um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Autoridade Nacional de Proteção de Dados (ANPD) é a agência reguladora vinculada ao Ministério da Justiça responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Para tanto, deve promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e medidas de segurança, bem como editar normas e orientação para que os agentes de tratamento possam se adequar à Lei.

PRINCÍPIOS APLICÁVEIS AO TRATAMENTO DE DADOS

Todas as atividades de tratamento de dados pessoais devem observar além da boa-fé, os seguintes princípios:

A **Finalidade** é aquilo que define para que o dado será tratado. O tratamento dos dados pessoais deve ser realizado para propósitos legítimos e específicos informados ao titular.

A **Adequação** define que deve haver compatibilidade do tratamento com as finalidades informadas ao titular.

O princípio da **Necessidade** prevê que o tratamento dos dados deve ser limitado ao mínimo necessário para a realização de suas atividades, ou seja, quando houver a coleta de dados para uma determinada finalidade deve-se perguntar o que é necessário para que seja possível atingir o objetivo? Coletar dados além o necessário é incompatível com a LGPD e traz mais riscos à Administração Pública, já que armazena dados desnecessariamente.

O princípio do **Livre Acesso** garante aos titulares a consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integralidade dos seus dados.

Já o princípio da **Qualidade dos Dados** é o que garante aos titulares a exatidão, clareza, relevância e atualização dos seus dados, de acordo com a necessidade para o cumprimento da finalidade do seu tratamento. Um exemplo é o armazenamento de currículo para uma vaga que só poderá ser preenchida para daqui a um ano. Os dados constantes do currículo já estarão desatualizados quando do preenchimento da vaga.

A **Transparência** é o princípio que garante aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

O princípio da **Segurança** determina que devem ser utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. É por meio deste princípio que fica claro que a Tecnologia da Informação e a LGPD devem ser integradas, pois não há como se falar em proteção de dados sem segurança da informação. Há várias medidas que devem ser utilizadas de forma a mitigar os riscos do vazamento de dados e é aqui que entra o princípio da **Prevenção**, já que é possível, após um mapeamento das atividades, adotar práticas que previnam a ocorrência de danos.

O princípio da **Não Discriminação** prevê que os dados não podem ser tratados para fins discriminatórios ilícitos ou abusivos.

Por fim, o princípio da **Responsabilização e Prestação de Contas** estabelece que os agentes deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

A partir desses princípios é possível verificar o quanto os titulares estão resguardados e o quanto que os agentes de tratamento devem se atentar quando da utilização dos dados pessoais.

A lei não prevê a impossibilidade de uso dos dados, ela busca oferecer mecanismos para que os dados sejam utilizados protegendo os direitos dos titulares.

BASES LEGAIS PARA TRATAMENTO DE DADOS

Para muitos, os dados só podem ser tratados se houver o consentimento do titular. Mas esse argumento não prevalece, já que o consentimento é o ato mais precário para o tratamento, bastando o titular revogá-lo para que o tratamento não seja mais realizado.

COMO DEVE SER OBTIDO O CONSENTIMENTO DOS TITULARES?

De acordo com a LGPD, para que o consentimento seja válido, é preciso que ele seja:

- Expresso – não existindo o consentimento tácito
- Livre – acabando com a autorização do tudo ou nada
- Inequívoco – não deve existir qualquer dúvida ou confusão
- Específico – a permissão serve apenas para aquela finalidade

Assim, a lei estabelece mais nove hipóteses de tratamento, em que não há a necessidade do consentimento pelo titular.

Para o cumprimento de obrigação legal ou regulatória pelo controlador. É aquela que deriva de uma lei ou outro instrumento fundamental em lei, não havendo necessidade do consentimento para o tratamento de dados, como por exemplo o E-SOCIAL, Receita Federal.

Pela Administração Pública, para o tratamento de uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. As políticas públicas são previstas em lei ou outros atos que as regulamente, não havendo que se falar em embasamento por esta base legal sem instrumento que a normatize. Pode ser citado como exemplo o transporte público, saúde pública.

Para a realização de estudos por órgão de pesquisas, garantida, sempre que possível, a anonimização dos dados pessoais. A LGPD trouxe o conceito de órgão de pesquisa em seu artigo 5º, XVIII, sendo que é considerado aquele órgão ou entidade da administração pública sem fins lucrativos cujo objetivo institucional é a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Não significa dizer que empresas privadas não podem fazer pesquisas, a questão é que esta base legal não as autoriza.

Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular de dados. Temos como exemplo a abertura de conta corrente, um pedido por aplicativo de *delivery* em que o titular pede uma comida, o que se busca é a entrega do que foi pedido. Assim o aplicativo deve cumprir a obrigação contratual em que eu estabeleci com ele e deve compartilhar os dados com outros envolvidos, como o restaurante e o motoboy que fará a entrega.

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa base legitima o direito de acesso à justiça sem precisar do consentimento da outra pessoa para que possa fazê-lo. Essa base legal também é utilizada para fundamento o armazenamento de dados para fins de defesa em processo judicial.

Para a proteção da vida ou da incolumidade física do titular ou de terceiros. É o caso de um atendimento médico de emergência ou em qualquer situação que a vida do titular ou de um terceiro estiver em iminente risco. É aquele cadastro de um sequestro, por exemplo.

Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Essa base legitima o tratamento para prestação de serviços essenciais à saúde como por médicos em hospitais para cirurgia de emergência.

Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. É uma base legal que precisa ser vista como muita cautela, pois o legítimo interesse do controlador não pode ultrapassar os direitos e liberdades fundamentais do titular dos dados. Não é uma base legal que pode ser usada como “coringa”, pois ela tem limitações.

Para a proteção de crédito. Essa base legal tem como fundamento reduzir o risco de inadimplência de pessoas físicas, quando essas requisitarem crédito. Então é autorizado que instituições financeiras tratem dados, para saber se a concessão de crédito é segura ou não, baseado no histórico da pessoa.

E OS DADOS SOBRE CRIANÇAS E ADOLESCENTES?

Dados sobre crianças e adolescentes também devem ser tratados com cuidado especial. De acordo com o Estatuto da Criança e do Adolescente, considera-se criança a pessoa até 12 anos de idade incompletos e adolescente, aquela entre 12 e 18 anos.

É necessário o consentimento expresso de um dos pais ou responsáveis e devem ser solicitados apenas os dados estritamente necessários para a atividade a ser realizada, sem repassar a terceiros. Se não houver consentimento, somente será permitido coletar os dados em casos de urgências, para contato com os pais ou responsáveis e/ou para proteção da criança e do adolescente.

Esse é um ponto que merece atenção, principalmente em relação aos jogos online, devendo o controlador realizar todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, considerando as tecnologias disponíveis.

QUAIS SÃO OS DIREITOS DO TITULAR DOS DADOS PESSOAIS?

Nos termos da LGPD, o titular dos dados pessoais tem direito ao acesso facilitado às informações sobre o tratamento de seus dados. Essas informações deverão ser disponibilizadas de forma clara, adequada e ostensiva.

A lei prevê que o titular tem direito de obter do controlador, que realize o tratamento de seus dados, a qualquer momento e mediante requisição:

- Acesso facilitado às informações sobre o tratamento de seus dados, especialmente em relação à confirmação da existência de tratamento e, em caso positivo, sua finalidade, forma, duração.
- Correção de dados incompletos, inexatos ou desatualizados.
- Anonimização, bloqueio ou eliminação de dados desnecessários.
- Portabilidade de seus dados.
- Revogação do consentimento/eliminação dos dados, sendo assegurado o direito de petição à autoridade nacional.
- Informação sobre o compartilhamento dos dados.
- Revisão sobre decisões automatizadas

PORQUE O TCEMG DEVE FAZER O CONTROLE DE DADOS PESSOAIS?

O TCEMG trata dados pessoais a todo momento - recebe, e é guardião, de um grande volume de dados pessoais, dos cidadãos, dos jurisdicionados e dos próprios servidores.

O tratamento de dados pessoais pode acontecer, a princípio, em quatro hipóteses: ações de controle externo, serviços à sociedade, ações de capacitação e ações administrativas internas.

O servidor quando analisa um processo de controle externo lida com vários dados pessoais e deve adotar práticas para que minimizem os incidentes, como não deixar a tela do computador aberta quando não estiver sentado em sua mesa. Adotar medidas de segurança é essencial para preservação dos dados.

O QUE É SEGURANÇA DA INFORMAÇÃO?

A Segurança da Informação é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os objetivos propostos e suas oportunidades. A Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo Políticas, normas, processos e procedimentos.

O QUE É POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?

A Política de Segurança da Informação do TCEMG é o conjunto de ações, técnicas, normas e boas práticas para o uso seguro de seus dados. Sua condução se orienta pelos seguintes princípios:

• **Autenticidade:** está associada à identificação de um usuário ou computador. Garante a legitimidade da identificação de uma pessoa ao acessar dados e informações.

• **Confidencialidade:** é a garantia de que somente pessoas autorizadas tenham acesso

às informações armazenadas ou transmitidas por meio de redes de comunicação.

• **Disponibilidade:** garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, ou seja, é a garantia de prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

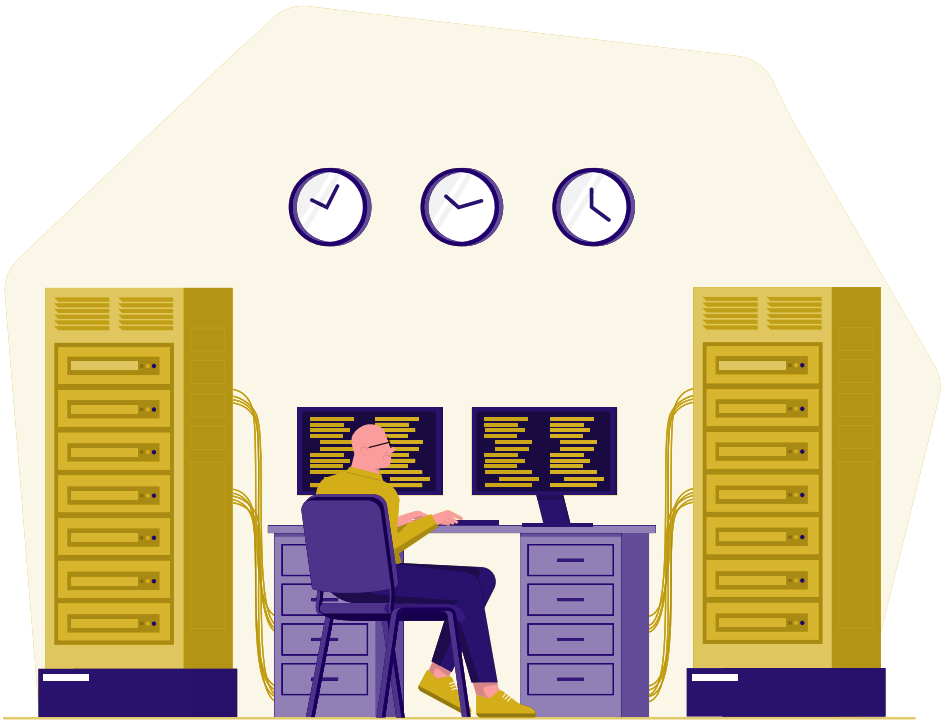
• **Integridade:** consiste na fidedignidade de informações. É a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

Qualquer indício de fraude, sabotagem, espionagem, desvio, falha, vazamento ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação caracteriza-se como um incidente de segurança da informação. Ele deve ser tratado de maneira rápida e eficaz para sanar as irregula ridades, registrando as ações para minimizar a sua ocorrência novamente.

O QUE É UMA ANÁLISE DE VULNERABILIDADES?

É a avaliação e identificação de falhas e potenciais ameaças de segurança numa infraestrutura tecnológica, como sistemas e equipamentos. Este procedimento permite antecipar problemas de cibersegurança que possam prejudicar a operação da instituição.



BOAS PRÁTICAS DE SEGURANÇA NO USO DOS RECURSOS DE TI

PROTEJA SEU E-MAIL

Use sempre seu e-mail institucional (usuario@tce.mg.gov.br) na comunicação oficial e procure não utilizar este e-mail em suas atividades, relacionamentos e tarefas de caráter pessoal. Lembre-se de colocar senhas nos dispositivos pessoais como celular, computadores e tablets e de jamais compartilhá-las.

CRIE UMA SENHA FORTE

Senhas seguras e fortes são compostas por, no mínimo, oito caracteres, combinando letras, números, símbolos especiais, maiúscula e minúscula. Para ajudar a lembrar, você pode utilizar uma palavra como base, mas substituir alguns caracteres. Por exemplo, em vez de usar tribunal como senha, utilize Tr13un@l.

CONTAS DIFERENTES, SENHAS DIFERENTES

O ideal e mais seguro é ter uma senha diferente para cada tipo de acesso ou serviço. Existem bons gerenciadores de senhas gratuitos, que podem te ajudar a não esquecê-las

PROTEJA SEUS DISPOSITIVOS

No seu computador, celular ou tablet, certifique-se que o antivírus esteja sempre atualizado e ative um bloqueio de tela e ainda criptografe os dados armazenados. Em todos os aparelhos, evite usar Wi-Fi público.

AUTENTICAÇÃO

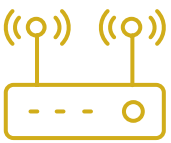
Se possível, utilize a sua assinatura eletrônica ou certificado digital, e ainda, se possuir, utilize o Token de autenticação de dois fatores para manter os seus acessos e documentos mais seguros.

NÃO ARMAZENE SENHAS NO SEU NAVEGADOR

Além de escolher senhas não óbvias, como sequências de números ou nome e sobrenome, tente não armazená-las nos sites, com aquele recurso de “manter-se conectado”. Em caso de invasão, seus dados ficarão expostos. Problemas também podem ocorrer ao esquecer de se desconectar da sua conta de e-mail ou redes sociais.

EM CASA, ALTERE A SENHA DA REDE WI-FI E DO MODEM

No modem, deve-se desativar a opção de WPS nas configurações. A conexão que utilizamos para gerir informação confidencial deve ser a mais segura possível.



CUIDADO COM OS LINKS

Evite clicar nos links de mensagens de remetente desconhecidos. Suspeite de softwares e links recebidos por e-mail em que você clica e não acontece nada.

REDES PÚBLICAS

Cuidado ao acessar rede wi-fi pública. Muitos estabelecimentos, como bares, hotéis, restaurantes e padarias, oferecem wi-fi de graça aos clientes. O acesso gratuito à internet desses locais públicos pode ser muito arriscado se você estiver acessando dados confidenciais de trabalho ou sites de banco ou de compras.

OUTRAS DICAS DE SEGURANÇA

• Não baixar ou instalar softwares de sites desconhecidos;

• Verificar se o endereço da página acessada inicia com “https://”. Isto significa que o site é seguro e tem um certificado digital válido;

• Ficar atento quando receber e-mails suspeitos de contatos inexistentes ou com nomes ou caracteres estranhos no campo do remetente;

• Não salvar arquivos com suas senhas de acessos a sistemas e aplicativos;

• Não compartilhar suas senhas. Elas são pessoais e intransferíveis;

• Não acessar promoções fantásticas divulgadas em sites com preços bem menores

do que os preços reais;

• Sempre bloquear seu computador quando não estiver em utilização ou for se ausentar da sua mesa;

• Manter seus dispositivos atualizados;

• Ter cuidado com pop-ups que surgem na tela quando se está navegando na internet. Com apenas um click eles podem instalar softwares maliciosos em sua máquina.

Um exemplo corriqueiro de má utilização de recursos de segurança é o uso do e-mail institucional em sites diversos, para realização de cursos, com a utilização da senha de acesso à rede do Tribunal. Isso pode trazer inúmeros riscos, pois, caso o site cadastrado possua algum agente malicioso, os dados institucionais estarão expostos.

DICAS PARA SERVIDORES NO TRATAMENTO DE DADOS

1. Ao tratar dados pessoais (independentemente de a quem pertençam, como foram obtidos ou onde são armazenados), observe as normas aplicáveis, bem como as políticas, orientações e boas práticas adotadas pelo Tribunal;

2. Certifique-se de usar apenas meios seguros e legais ao tratar dados pessoais;

3. Certifique-se de tratar dados pessoais apenas para fins legítimos e restritos à

finalidade pública e ao interesse público, isto é, para cumprimento de competências legais, atribuições do serviço público ou de políticas públicas;

4. Proteja os dados pessoais com cuidado;

5. Não colete informações desnecessárias;

6. Trate dados apenas na medida necessária para realização do serviço de sua atribuição;

7. Reduza os riscos relacionados à segurança da informação;

8. Ao tomar ciência de uma falha de segurança, reporte ao Núcleo de Proteção de Dados Pessoais;

9. Seja cuidadoso ao discutir assuntos que envolvam dados pessoais com indivíduos de fora da instituição;

10. Evite conversas em locais públicos ou de uso coletivo (elevadores, saguão, corredor), que tenham como objeto dados pessoais;

11. Não use dados pessoais desatualizados ou inexatos;

12. Previna a perda acidental ou destruição de dados pessoais;

13. Evite o acesso não autorizado aos dados controlados pelo Tribunal de Contas;

14. Limite o acesso aos dados pessoais apenas aos agentes que necessitem desses para as atividades da administração pública do Tribunal de Contas;

15. Reporte ao gestor e ao Núcleo de Proteção de Dados Pessoais a ocorrência de violações à LGPD;

16. Não envie e-mails para pessoas ou grupo maior do que o necessário. Cuide para quem você irá enviar o e-mail ou cópia desse quando houver dados pessoais;

17. Não deixe documentos com dados pessoais na impressora, copiadora, fax ou na sua mesa, onde outros podem ver. Também não deixe sua tela do computador aberta com dados pessoais, quando você não estiver utilizando o computador;

18. Verifique a existência de salvaguardas quando for compartilhar dados com terceiros;

19. Não tire fotos ou filme documentos que contenham dados pessoais;

20. No desenvolvimento de novos sistemas, processos ou procedimentos que envolvam o tratamento de dados pessoais, adote medidas de proteção de dados desde a concepção até a execução;

21. Proceda com a correção de dados pessoais que estejam imprecisos, incorretos

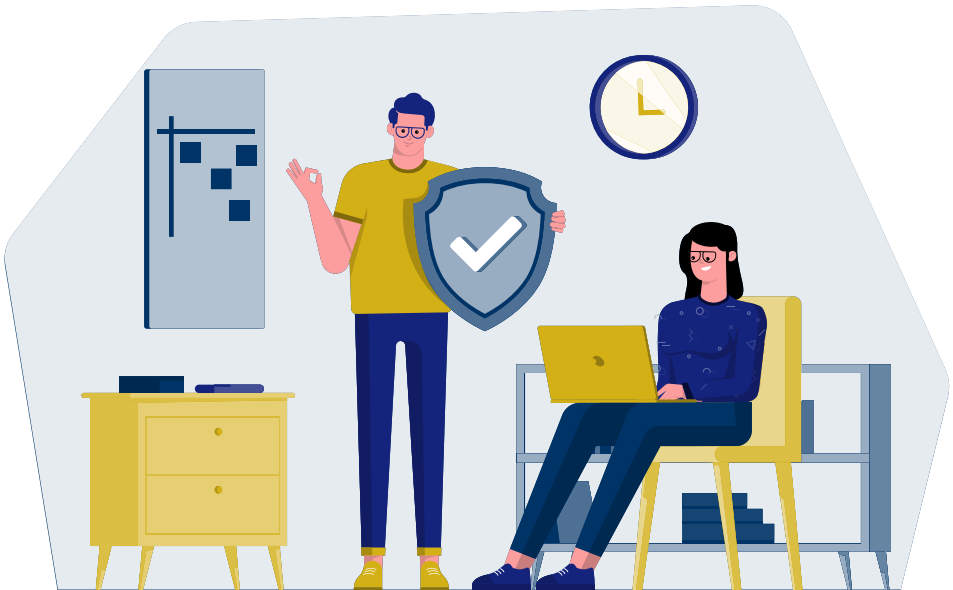
ou incompletos;

22. Garanta que os titulares dos dados tenham a possibilidade de revisar e corrigir seus dados pessoais;

23. Em conformidade com normas específicas, guarde os dados apenas pelo tempo necessário;

24. Elimine os dados que não possuam mais justificativa para que sejam mantidos e tratados pela instituição;

25. Forneça explicações ao titular sobre a utilização dos dados.



TRIBUNAL DE CONTAS DO ESTADO DE MINAS GERAIS

Av. Raja Gabaglia 1.315 - Luxemburgo - Belo Horizonte - Minas Gerais
CEP: 30380-435 | Tel: (31) 3348-2111

www.tce.mg.gov.br

@TCEMGoficial ***@tcemg*** ***/tcemgoficial*** ***@tcemgoficial***